Telecommunications Industry Ireland submission to public consultation on National Cyber Security Strategy 2019-2024 Midterm Review

7 February 2023

Introduction

Ibec's Telecommunications industry Ireland welcomes the opportunity to respond to the National Cyber Security Strategy 2019-2024 Midterm Review Consultation Paper. Its members are the key players in the telecommunications sector, who account for the vast bulk of industry investment and employment.

Telecommunications is the backbone of Ireland's digital economy and underpins it. Cyber security is essential to both. In 2020 the OECD. recognised Ireland as one of several 'global hubs of digitally delivered services'. Some 240,000 are employed in digitally intensive sectors, up 17% since 2016, and an estimated 30% of data held in the European Union (EU) is held in Ireland.

It is also very important for our future competitiveness that Ireland is able to compete for the forecasted €12 trillion of global economic output enabled by 5G in the period to 2035. Adequate cyber security will be absolutely essential to this.

The telecoms sector itself employs 25,000 people, made a network investment of approximately €3.3 billion over the past 5 years, paid €932 million for spectrum over the last 10 years, and is estimated to contribute c.€2.5 billion to the economy annually.

National Capacity Development [page 16-17, Consultation Paper]

Telecommunications Industry Ireland has for many years urged a substantial increase in the resourcing of the National Cyber Security Centre (N.C.S.C.) in its pre-budget submissions and at meetings with key stakeholders. This is because the telecommunications industry understands the vital strategic national importance of cyber security.

We recommend, as Ibec does, that Ireland invests further in national cyber security capacities and continues to play a strong role internationally in these areas. We recommend that as a nation Ireland engages, co-ordinates and strengthens our cyber security ecosystem. Research by William Fry and Amárach highlights that data-driven regulatory issues have become a major investment attractor. Consequently, Telecommunications Industry Ireland:

- Welcomes the Government expansion of the N.C.S.C. to date.
- Supports further and appropriate resources for national cyber security capacities, as signalled in our on-going stakeholder engagement and pre-budget submissions. Further resources will be necessary to fulfil (a) the recommendations of the N.C.S.C. Capacity review, the N.C.S.C. activities proposed in the mid-term review and the proposed expansion of N.C.S.C. functions in response to upcoming EU requirements e.g., the revised EU Network and Information Security Directive (N.I.S. 2); and (b) the Commission on the Defence Forces' recommendations accepted by the Government.

While the telecommunications sector invests heavily in cyber security, certain essential functions in this regard can only be discharged by the State. The adequate discharge of these functions is essential to protect both citizens and the digital economy and requires appropriate resources in the N.C.S.C.

The telecommunications sector works in close cooperation with the N.C.S.C. and looks forward to the continuation of this relationship. It supports the following proposals contained in the Consultation Paper:

- Increase the N.C.S.C.'s ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks through a variety of means, including the continued development of its Sensor network across the systems of public bodies, critical infrastructure, and other relevant constituents, underpinned by clear legal powers.

- The establishment by the N.C.S.C. of a national Coordinated Vulnerability Disclosure (C.V.D.) policy, including a role for the N.C.S.C. to act as a coordinator and trusted intermediary between researchers and industry as required under the revised N.I.S. 2 Directive.

- The N.C.S.C. will further enhance its existing Active Cyber Protection 2 measures to identify vulnerable systems and engage with owners of critical infrastructure on remediation.

Advanced consultation with the telecommunications industry is requested regarding the above proposals insofar as they directly affect the sector.

Critical National Infrastructure Protection [page 18-20, Consultation Paper]

Telecommunications industry Ireland welcomes the progress to date on critical national infrastructure [C.N.I.]. These include the following:

- The deployment and development of the critical national infrastructure [C.N.I.] protection system flowing from the N.I.S.2 Directive.
- The publication by the N.C.S.C. of guidelines for operators of essential services [O.E.S.] and its engagement with them to identify and mitigate cyber risks affecting designated services, including through a programme of security audits.
- The development of national legislation for critical national infrastructure will be addressed through the transposition of the N.I.S.2 Directive.
- In respect of telecommunications infrastructure, the government has endorsed the EU's 5G Security Toolbox as the framework for which Ireland will secure its next generation electronic communications networks. A series of electronic security control measures have been drafted in consultation with industry, and legislation has been brought before the Oireachtas to establish a legal basis for these controls.

The Minister has recently published primary legislation on 5G security to assess the risk profile of providers of electronic communications network equipment and, if required, to designate certain vendors as being high risk. The Committee stage amendment to the Communications Regulation Bill 2022 will also provide for certain parts of electronic communications networks to be designated as being critical and certain powers which would ensure that high risk vendors would not be used in critical electronic communications networks.

Industry is broadly understanding of the grounding of the sections of the Communications Regulation Bill 2022 on high-risk vendors. Telecommunications network operators are committed to a risk and evidence-based, vendor-neutral approach that includes vendor agnostic security assurance and increased vendor diversity.

It is understood by industry that EU Member States are required to implement the 5G Toolbox and are evaluating suitable frameworks to assess the risk profiles of suppliers and relevant restrictions. In situations where change is in the national interest the best approach affords reasonable flexibility in

terms of how this is achieved. To the maximum extent possible the approach should be based on technical specifications. In this regard the range of approaches implemented in various other EU Member States offer useful learnings, particularly by those with very significant capabilities and expertise (e.g. France, Germany etc.).

Network operators take the security of their networks very seriously and are compliant with all relevant EU and Irish guidelines and standards. Network security is a central consideration when companies are designing and building their networks and is a major investment priority. As additional compliance measures will incur additional costs and resources, and may impact end customers service and pricing, Telecommunications Industry Ireland therefore requests that best endeavours are made to ensure that the implications of these future requirements are aligned with current best practices.

It is essential that there is full advance consultation with Telecommunications network operators on any proposals or Government mandated changes which may impact on network operations or the rollout of telecommunications network infrastructure to avoid a risk of service interruptions or increased costs to consumers. The implications for the pace of rollout of high speed fixed and mobile networks must be considered, and any other knock-on effects avoided.

As stated in the Telecommunications Industry Ireland submission to the public consultation on the Electronic Communications Security Measures, any new tests or standards must be objective, transparent, proportionate, and reasonable, and should be subject to a public consultation.

Clarity is needed by industry regarding the scope of the Committee stage amendments to the Communications Regulation Bill, 2022. Are both fixed and mobile networks affected and how far is it proposed to go beyond the core? Clarity is also needed on exactly what network components come within the scope of these amendments. The definition of 'critical components' should be limited to core network equipment. The overall approach should be based on the approach in the 5G Toolbox and a list of 'critical components' should be made available as soon as possible. Clarity is needed by industry regarding the scope of the legislation. Does it include both fixed and mobile networks. Is it proposed to go beyond the core and, if yes, how far?

It is essential that there is detailed consultation with the telecommunications industry regarding such issues as timeframe, transition, implementation, contractual agreements, and compensation.

Telecommunications industry Ireland welcomes the following proposals contained in the Consultation Paper:

- The N.C.S.C. will begin offering a vulnerability assessment service to critical infrastructure and government entities in 2023.
- The N.C.S.C. will begin the process of creating a database of critical infrastructure, vendors, and managed services.
- The N.C.S.C. will build a network of sectoral Information Sharing Networks…..enhancing the security and resilience of critical infrastructure. This Information Sharing Network will be prepared for, and can coordinate during, a major cyber security incident.
- The N.I.S. Competent Authority role for critical infrastructure operators will be further federated, with sectoral regulators integrating cyber security compliance to their existing regulatory roles, thereby enabling the N.C.S.C. to focus on its core mission, while at the same time providing expert guidance to those regulators.

Telecommunications industry Ireland requests clarification on sectoral regulation and if ComReg will assume responsibility for all cyber security regulation for the sector. It also strongly recommends that a single standardised format for incident reporting be used by all regulatory entities. The timing of updates on incidents required of the telecommunications industry by all such entities should also be aligned.

Public Sector Data and Networks (pages 21-23, Consultation Paper)

The telecommunications sector looks forward to the publication, envisaged in the first quarter of 2023, of recommendations for the procurement of software, hardware and cloud computing services on Government IT and telecommunications infrastructure. It will engage with the N.C.S.C. as appropriate regarding recommendations relevant to the sector.

It notes that it is intended that relevant provisions extending the "Sensor" programme to other public bodies and to critical national infrastructure will be included in the draft Heads of Bill which are to provide relevant legal powers for the N.C.S.C. Advanced consultation with the telecommunications industry is requested regarding provisions of this legislation insofar as they directly affect the sector.

Should there be a requirement for the entities providing cyber security services to the public sector in Ireland to be accredited against a standard to be developed by the N.C.S.C., consultation with industry is recommended.

Citizens [page 33-35, Consultation Paper]

Telecommunications industry Ireland welcomed the establishment by Minister Ossian Smyth of a ComReg facilitated Nuisance Communications Industry Taskforce and its members are very active participants in its work. While initial measures are in prospect to address the issue of fraudulent calls and text messages, in the long term technically more complex measures will probably be required. The latter will be quite expensive for industry to implement but probably necessary because of the increasing sophistication of fraudsters.

It is essential that regulatory policymakers and regulators accept the reality that profitability by telecommunications companies is essential to funding such investment in measures to deter fraudulent calls and text messages, and indeed to funding investment in cyber security more generally. Unless all telecommunications operators, both large and small, are allowed to generate the necessary resources through operational profitability the telecommunications industry will not be able to significantly hinder the current threat, much less the type of sophisticated threat likely to emerge in the near future.

Governance Framework and Responsibilities [page 35, Consultation Paper]

Telecommunications Industry Ireland welcomes the proposal contained in the Consultation Paper to establish an Advisory Group to provide the N.C.S.C. with independent perspectives and input on strategy and policies. It is essential that the telecommunications sector is adequately represented on the Advisory Group so that the unique and essential perspective of the sector can be conveyed.

Further information

For further information please contact:

[redacted]
Director
Telecommunications Industry Ireland
Ibec
84-84 Lower Baggot Street
Dublin 2

Email: [redacted]